Economic Modeling of a Trust Network via Positive Collusion and Aspiration Adaptation

Jin-Hee Cho and Ananthram Swami
Computational and Information Sciences Directorate
U.S. Army Research Laboratory
{jinhee.cho, ananthram.swami}@us.army.mil

Key words – economic modeling, trust network, positive collusion, aspiration, rationality, wireless mobile networks

Abstract – Military communities in tactical networks must often maintain high group solidarity based on the trustworthiness of participating individual entities where collaboration is critical to performing team-oriented missions. Group trust is regarded as more important than trust of an individual entity since consensus among or compliance of participating entities with given protocols may significantly affect successful mission completion. This work introduces a game theoretic approach, namely *Aoyagi*'s game theory on collusion in a dynamic Bertrand oligopoly. This approach improves group trust by using positive collusion encouraging unanimous compliance with a given group protocol. Further, inspired by aspiration theory in social sciences, we adjust the expected system trust threshold level that should be maintained by all participating entities to effectively encourage benign behaviors. The results show that there exist optimal settings (e.g., system trust threshold level) that can maximize group trust level while meeting required system lifetime (survivability).

1. Introduction

Collaboration is critical in team-oriented missions. This is particularly important in military communities engaged in tactical operations, where it is important to maintain group solidarity based on the trustworthiness of the individual entities. Communal compliance to a common protocol can significantly affect successful mission completion. As such, group trust is often considered to be more important than the trust of any single entity. Rewards and penalties are a natural way of enforcing or encouraging behaviors. In this work, we introduce a game theoretic approach, namely *Aoyagi*'s game theory [1] to collusion in a dynamic Bertrand oligopoly.

This approach improves group trust by using positive collusion to encourage unanimous compliance with a given group protocol. That is, the entire system is penalized or rewarded regardless of which individual entity misbehaved or behaved. Ng and Seah [5] used *Aoyagi*'s game theory to improve cooperation of nodes where nodes are more likely to be selfish in resource-restricted wireless networks such as mobile ad hoc or sensor networks. However, [5] only deals with a node's selfishness by examining the behavior of packet forwarding or dropping. Our work examines more aspects of an entity in order to assess its trustworthiness derived from a composite network considering the characteristics of communication, information, social, and cognitive networks.

Aspiration is a popular concept employed in diverse fields to encourage performance of an organization or individual entity by using it to determine "success" or "failure." The underlying idea is that entities work hard to avoid failure where failure is defined as being below the aspiration level, a standard set implicitly or explicitly by peers or the community at large. For example, aspiration theory has been used in fields such as education [6], economics [3], organization management [4], computer science (artificial intelligence) [7], and others in order to facilitate persistent endeavor of participating entities to improve their performance.

This work also utilizes the concept of "aspiration level" as an expected group trust threshold that can be optimized for all entities in order to maximize group trust level while meeting required system survivability. We developed a mathematical model using Stochastic Petri Nets (SPN) to describe the proposed group trust framework for a tactical wireless mobile network having severe resource constraints. We discuss the performance metrics obtained through the evaluation of our SPN model, and provide physical interpretations based on the insights derived from economic modeling perspectives. The results imply that a system designer can fine-tune the trust threshold so as to meet required system survivability as well as to maximize group trust level.

2. Protocol Design and Assumptions

In this section, we provide an overview of the proposed protocol design based on *Aoyagi*'s game and aspiration theories, along with the assumptions made in the proposed protocol.

Aoyagi's game is a repeated game where each player reveals its private signal publicly at the end of each stage. For example, in an oligopoly, the products of the sellers are not distinguishable to the buyers. If one seller reduces an item's price, then other sellers will have a reduced demand due to the price cut. So, in this market, all sellers are supposed to follow the price that is determined by the market. Thus, if all players say "yes" signals publicly at the end of each game period, it means all players unanimously preserve the market price. Then, all players do not face any penalty by violating the rule. However, if any one of the payers says "no" meaning "I am not following the rule, I am offering a lower price to buyers," then all players may face a penalty due to the individual player's action. The main issue in this game is whether the publicly revealed signals of the sellers (i.e., actual prices offered to buyers) are true. Sellers may say "yes" representing obedience to the rule, but they may offer a lower price to attract more customers than other companies (e.g., OPEC in the 80's). Therefore, in this game, it is important to build a protocol under which everyone has an incentive to tell the truth. That is, when a player lies, then she should be penalized in some way so that she is incentivized to tell the truth to avoid the penalty.

In our proposed protocol, we also follow a similar rule such that "all nodes maintain a trust threshold that is expected by the system" (e.g., system trust threshold for mission execution). The targeted network environment is a wireless mobile tactical network where a commander collects trust values of all participating nodes based on public signals disseminated by each node. Public signals from nodes indicate whether it is observing the trust threshold level, and are assumed to be true. Only when all nodes publicly say they are observing the trust level (the so called "collusion phase"), do they not receive any penalty. However, a rational node may lie to avoid the penalty. That is, a node may say "yes" but the node may lie by not actually maintaining the expected trust level. Further, a node may not follow the rule in order to achieve its attack goals if it is an attacker. To alleviate this effect, we employ a distributed voting-based intrusion detection system (IDS) [2]. Excluding false negatives (a liar is not captured by the IDS) and false positives (a good node is falsely diagnosed as bad by the IDS), when any liars are detected, the system will be penalized by evicting a certain portion of nodes with the lowest trust values, endangering system survivability. We define "system survivability" or "lifetime" as the time when a certain fraction of participating nodes in the system die or are evicted, e.g., one third of nodes should be alive as group members. We call this penalty a *high penalty* since a node is lying in addition to not maintaining the given trust threshold level. If a node is not maintaining the trust level but it does not lie, saying "no" for the public signal, then it will face the penalty phase but, depending on the degree of its rationality, it can be penalized or redeemed. We define "rationality" of a node as the degree of the willingness to follow the given protocol. However, since this node at least did not lie, we penalize the system with a *low penalty*, evicting a fewer number of nodes with the lowest trust values than that evicted by a high penalty. Note that an *individual* node's misbehavior causes the *system* to be penalized, ultimately resulting in reducing system survivability.

Our goal is to identify the optimal trust level, mimicking what aspiration level can improve the performance of employees in an organization [4]. We observe that there exists the tradeoff between maintained trust level and system survivability. If the trust threshold is high, the system is more prone to be penalized; it will take a longer time for the system to reach this trust level, and more nodes are likely to be evicted in this longer convergence period. Consequently, system survivability will be low. However, the efforts to reach the trust threshold will allow individual entities to grow their trust level ultimately.

We have developed a mathematical model using SPN where the underlying model is *Markov* or *semi-Markov* for efficiently representing a large number of states. In this paper, we only demonstrate the results obtained through our analytical model. The details of our model will be included in the journal version of this paper.

We evaluate the proposed protocol with two metrics: trust level and survivability probability.

Trust Metric

We consider the four types of trust derived from four different network layers: communication, information, social, and cognitive networks in order to assess a node's trustworthiness. We measure *communication trust* based on a node's degree of *cooperativeness* (e.g., packet dropping or forwarding) and *energy* (i.e., remaining energy). *Information trust* of a node is measured based on the degree of *data integrity*, whether a node modifies or forges messages. *Social trust* is assessed based on the degree of *honesty*, whether a node lies or disseminates fake information. *Cognitive trust* is measured by the degree of rationality where rationality is defined as the degree of willingness to follow the given protocol. Note that rationality is affected by environmental conditions such as energy in this work.

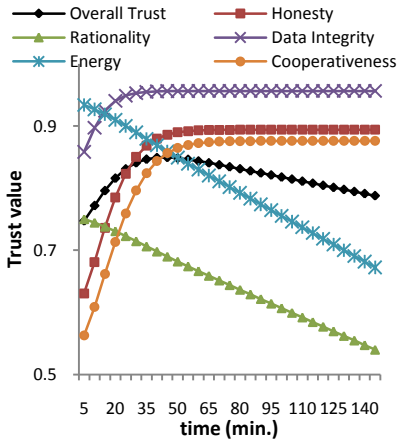

Figure 1: Average Trust Values with respect to Each Trust Component with the Trust Threshold (T_{th}) = 0.7 and Initial Trust Distribution with [0.5, 1].

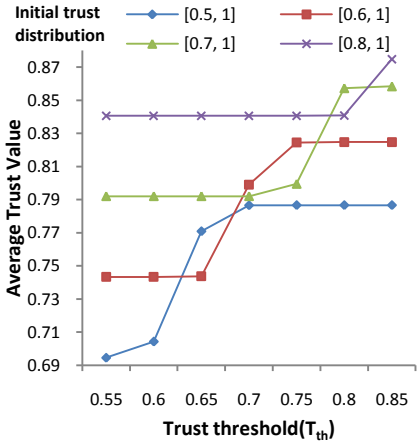

Figure 2: Average Trust Values with respect to Varying the Trust Threshold (T_{th}).

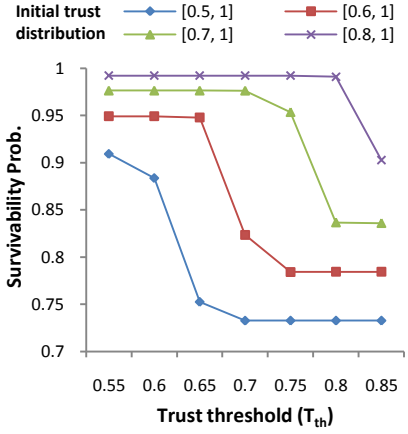

Figure 3: Survivability Probability vs. Trust Threshold (T_{th}).

We associate the rationality of a node with its remaining energy reflecting the phenomenon that an entity becomes generous under less stressful conditions such as high remaining energy. Further, we link a node's behaviors such as cooperativeness (e.g., less cooperative behavior saves a node's energy) and data integrity (e.g., frequent message modification may consume more energy than simply forwarding messages) with the remaining energy. In addition, we also relate a node's rationality with willingness to improve other trust components such as cooperativeness, honesty, and data integrity. That is, a node with high rationality will change its behaviors more aggressively to improve other trust components. The overall trust is the weighted sum of all five trust components with an equal weight. The detailed trust metric equation will be provided in the journal version.

Survivability Probability

We define the survivability probability of the system as the time-averaged probability that more than one third of the initial member nodes are alive for mission execution. Note that our goal is to identify an optimal trust threshold to meet the two conflicting two goals - system trust level and survivability requirements.

3. Numerical Results and Analysis

We show results obtained from the evaluation of our developed analytical models using SPNs. Figure 1 first shows how each trust component value and the overall trust of an individual node changes over time. We observe that while the degree of honesty, data integrity, and cooperativeness initially increased significantly over time, the overall trust decreased as time progresses sufficiently due to energy depletion and also the reduced degree of rationality (which is also affected by exhausted energy level). Figures 2 and 3 show the tradeoff between average system trust level and system survivability. We varied the initial trust distribution of participating nodes based on the uniform distribution with various lower bound ranges to see their impact on both metrics. As the trust threshold level increases, average trust levels improve while system survivability decreases due to higher chances of "misbehaving nodes" and, hence, higher penalties until the system reaches the trust threshold level.

4. Conclusions and Future Work

We used Aoyagi's game theory and aspiration theory in order to model a tactical network where a commander node collects and computes self-reported trust levels of participating member nodes for mission assignment and execution. In particular, we developed a composite trust metric whose components are derived from characteristics of communication, information, social, and cognitive networks for trust evaluation. We adopted the scenario used in Aoyagi's game theory in which the commander asks all participating nodes to maintain a certain trust threshold and penalizes them upon lack of consensus in following the trust threshold. Given this scenario and various operational and environmental network conditions, we indentified an optimal trust threshold that can maintain desired system trust levels while meeting system survivability. A system designer can dynamically select a trust threshold with the goal of achieving both high system trust and required system survivability.

Our future work will include (1) examining other key design parameters that affect trust levels and system survivability such as trust update interval; (2)

investigating how payoffs by an individual entity's decision making are maximized based on different trust thresholds; and (3) comparing the proposed model with other models that have different decision rules.

References

[1] M. Aoyagi, "Collusion in Dynamic Bertrand Oligopoly with Correlated Private Signals and Communication," *Journal of Economic Theory*, vol. 102, no. 1, pp. 229–248, Jan. 2002.

[2] J.H. Cho and I.R. Chen, "Model-based Evaluation of Distributed Intrusion Detection Protocols for Mobile Group Communicating Systems," *Wireless Personal Communications*, 2010.

[3] E. Diecidue and J. Ven, "Aspiration Level, Probability Of Success And Failure, And Expected Utility," *Int'l Economic Review*, vol. 49, no. 2, pp. 683-700, 2008.

[4] H. R. Greve, "Sticky Aspirations: Organizational Time Perspective and Competitiveness," *Organization Science*, vol. 13, no. 1, Jan.-Feb. 2002, pp. 1-17.

[5] S. K. Ng and W. K. G. Seah, "Game-Theoretic Approach for Improving Cooperation in Wireless Multihop Networks," accepted to *IEEE Transactions on Systems, Man, and Cybernetics-Part B: Cybernetics*, 2010, [Online] version available.

[6] R. J. Quaglia and C. D. Cobb, "Toward a Theory of Student Aspirations," *Journal of Research in Rural Education*, vol. 12, no. 3, pp. 127-132, Winter 1996.

[7] K. M. Sim and S. Y. Wang, "Flexible Negotiation Agent with Relaxed Decision Rules," *IEEE Transactions on Systems, Man, and Cybernetics-Part B: Cybernetics*, vol. 34, no. 3, pp. 1602-1608, June, 2004.